Tutorial – Hand Geometry

Introduction:

Biometrics are best defined as the science of using unique physiological or behavioral characteristics to verify the identity of an individual. Biometric characteristics are unique to individuals and cannot be lost or stolen like passwords, making them not only convenient but also more effective in the prevention of theft or fraud. They include fingerprints, iris scanning, hand geometry, voice patterns, facial recognition and other techniques. Biometrics are of interest in any area where it is important to verify the true identity of an individual.

Biometrics are not a panacea for all our personal identification related issues, but an enhancing tool in our technology toolbox. A great amount of technical progress has been made, providing more accurate and more refined products. The unit cost is dropping to a level, which makes them suitable for broader scale application. The knowledge base concerning their use and integration into other processes has increased dramatically.

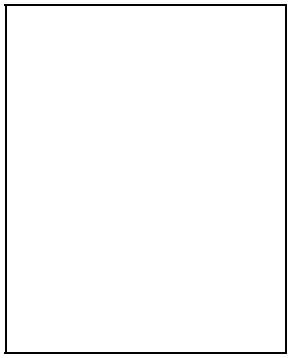
Currently, these techniques are employed in a much broader range of public-facing situations, one of which is hand geometry. This technology employs the use of a sensor, algorithm, and matcher technology to verify the identity of an individual. This tutorial will primarily discuss this technology.

Types of Authentication Methods:

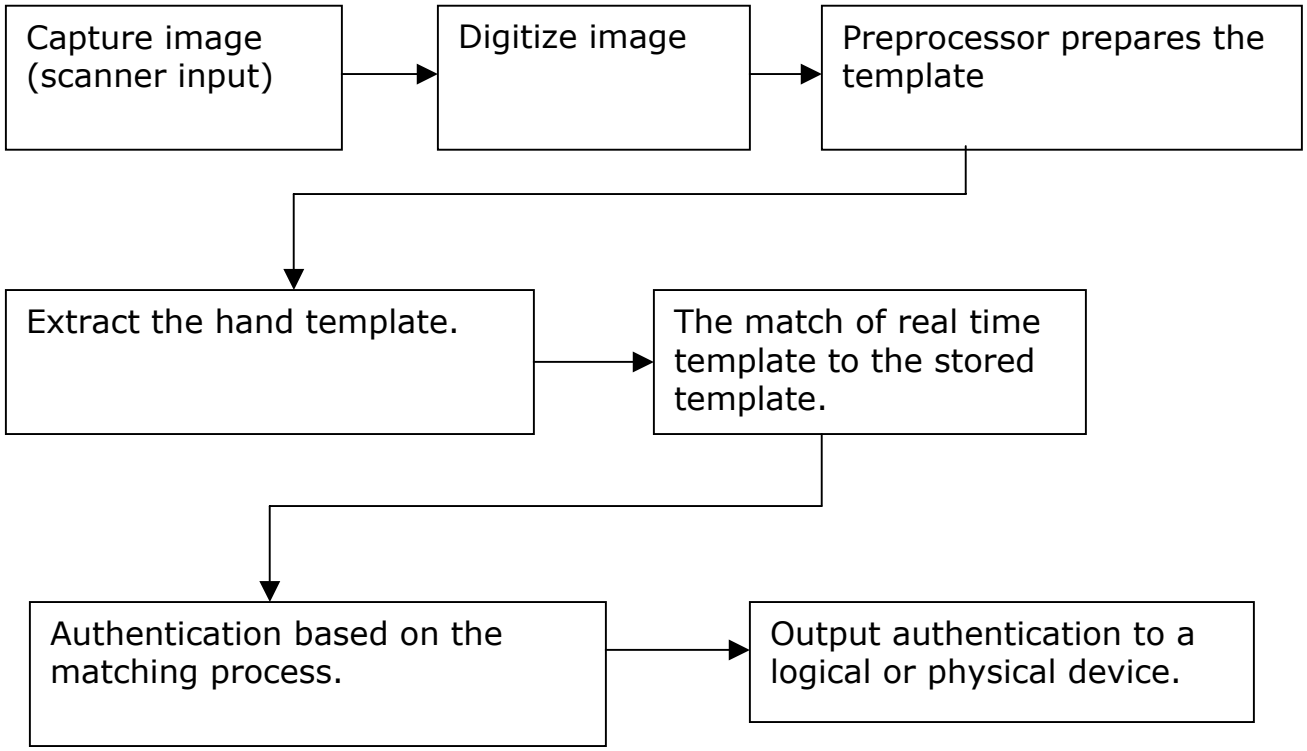
The two types of authentication are "Identification" and "Verification". These are sometimes confusing to people when discussing biometrics. The majority of biometric devices operate in the verification mode. The means that an identity is proven by calling a particular template from storage (invoked by the use of PIN, token or user-id) and then the person presents the live sample of their biometric for comparison, which results in a match or no match according to the predefined threshold parameters. This is known as a one-to-one (1:1) method of verification that may be performed quickly as the result of comparing the template to live sample/biometric.

The other match is a one-to-many (1:m), which is where the person submits their biometric for identification and the system attempts to identify the person from a database of templates. The user presents the biometric sample and the database engine starts the search. The system will search to find the correct identified person that matches the live sample. The one-to-many methodology operational speed is based on the biometrics used and the size of the database.

Using the one-to-one methodology will be faster than the one-to-many. The search is limited and the comparison is only against a limited number of templates.



Hand geometry Overview:



As the name suggests, hand geometry is concerned with measuring the physical characteristics of a user's hand from a three-dimensional perspective. One of the most established methodologies, hand geometry offers a good balance of performance characteristics and is relatively easy to use. This methodology may be suitable in cases where a large user base may access the system infrequently and may be less disciplined in their approach to the system. If desired, accuracy can be very high while flexible performance tuning and configuration can accommodate a wide range of applications. Hand geometry readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Hand geometry is an obvious first step for many biometric projects due to its ease of integration into other systems and processes, coupled with its ease of use.

Hand Geometry Systems:

There are only two major vendors in this biometric methodology at this time. Recognition Systems, Inc uses hand-scan technology and Finger geometry is led by Biomet Partners.

The scanner consists of a light source, mirror, camera, and a scanning surface. The hand scan input device is a 32,000-pixel charged coupled device digital camera, inferring the finger length, width, thickness, and curvature for the purposes of verification, but not for identification. The scanning device takes over 90 measurements and then the hand and fingers characteristics are represented as a 9-byte template.

Hand geometry processes the scanning of the hand's 3-D features, such as the size and shape of the knuckles or fingers. The system disregards any scars, cuts, etc. To keep the hand in one uniform position, pegs are used to signify where the area between the fingers should be placed.

The finger geometry technology is similar, but draws on the shape and characteristics of the index and middle finger. The data that is saved is on 20-byte template.

The scanners are non-threatening, fast and accurate, and work equally well with the right or left hand. Hand-scan is occasionally

misunderstood as "palm reading", due to the fact that the hand is placed palm-down on the reader.

In many situations it is desirable to have a biometrics system that is sufficient for verification, thus hand geometry. Fingerprints are used for infrequent identification, while hand geometry is used for frequent verification.

Hand Geometry Process:

The process for capturing the biometric sample is straightforward. The user to enroll places their hand, palm down on the systems reader surface. The user then aligns their hand with the pegs designed to indicate the proper location of the thumb, forefinger, and middle finger. The placement is required so that the enrollment can properly take place. The system requires that a user perform three placements on the device to produce an enrollment template. The enrollment template is a representation of the best data from the three placements of the person.

The hand-scan or finger scan is relatively accurate technology. The systems both perform the 1-to-many search on the template database.

The template can be referenced with a Pin, Token, or other means of identification in order to recall it for comparison with the live sample. If the database uses one-to-many matching, then no other items are linked to the template. The enrollment process and quality of the template are critical factors in the overall success of the biometric application. If a poor template is generated by the capture during the enrollment process, the subject will be required to re-enroll.

The templates can be stored in a variety of applications. The template can be stored on the biometric device or a central repository (server or web). There are advantages and disadvantages to both of these methods. If the biometric is stored on the device, it will be faster and self-containing; however, the templates can become vulnerable to other forces such as if the device fails. Then there will be a need to reload the template database or re-enrolling the users.

If storing the templates in a central repository is the option, it will provide an additional level of security to the network. Each template can vary between 9 bytes and 20 bytes. If the network fails and access to the central repository is unavailable, access to a system or a

door could be denied. There are methods to utilize in order to avoid an "access denied" by the authorized users.

The biometric template should be encrypted during storage and transmission of the template. This provides a level of security that truly enhances any physical or logical access program for an organization.

Areas of concern:

There are some areas of concern using hand geometry, as there would be when putting any system into an application.

Hand geometry is a design that has been unchanged for years. The size of the units prevents it from being used in most logical access scenarios.

Injuries to a person's hand or hands can cause the user to be rejected falsely. Injuries to the hands are fairly common and could make the use of hand geometry impossible.

Each application needs to be reviewed based on the facts and the use of biometrics. There may be concerns but with proper preparation and using the correct solutions the concerns may be overcome.